

IN THE CLAIMS:

1. (Currently amended) A method, in a computer system, for monitoring data sent from a the computer system, comprising:
detecting a request for an outgoing transfer of data from a program in the computer system to a destination;
determining whether the destination is a trusted site; and
performing a corrective action if the destination is not a trusted site, wherein the step of performing a corrective action comprises changing the destination of the outgoing transfer to the computer system, and determining whether the program operates in response to the changed destination.
2. (Original) The method of claim 1, wherein the step of determining whether the destination is a trusted site comprises matching the destination against a list of trusted sites.
3. (Original) The method of claim 1, wherein the corrective action comprises blocking the outgoing transfer.
4. (Currently amended) The method of claim 1, wherein the corrective action comprises disabling the program that requested the outgoing transfer of data.
5. (Cancelled)
6. (Currently amended) ~~The method of claim 1~~ A method, in a computer system, for monitoring data sent from a computer, comprising:
detecting a request for an outgoing transfer of data from a program in the computer system to a destination;
determining whether the destination is a trusted site; and
performing a corrective action if the destination is not a trusted site, wherein the step of performing a corrective action comprises:

~~irreversibly~~ encrypting the data; and

determining whether the program operates in response to the encryption.

7. (Currently amended) The method of claim 6, wherein the step of ~~irreversibly~~ encrypting the data comprises irreversibly encrypting the data by injecting random numbers into the data.

8. (Currently amended) ~~The method of claim 1, further comprising:~~ A method, in a computer system, for monitoring data sent from the computer system, comprising:

detecting a request for an outgoing transfer of data from a program in the computer system to a destination;

determining whether the destination is a trusted site;

performing a corrective action if the destination is not a trusted site;

determining whether the amount of data for the outgoing transfer is uncharacteristically high; and

performing a corrective action if the amount of data is uncharacteristically high.

9. (Currently amended) The method of claim 1, further comprising:

determining whether the data includes personal information if the destination is a trusted site; and

performing a corrective action if the data includes personal information.

10. (Original) The method of claim 9, wherein the step of determining whether the data includes personal information comprises performing a text string search or binary pattern search on the data.

11. (Original) The method of claim 1, wherein the step of performing a corrective action comprises storing a log of the outgoing transfer.

12. (Original) The method of claim 11, wherein the step of storing a log of the outgoing transfer comprises storing the data.

13. (Original) The method of claim 11, further comprising transferring the log to a remote computer.
14. (Currently amended) A method, in a computer system, for monitoring data sent from a the computer system, comprising:
- detecting a request for an outgoing transfer of data from a program in the computer system to a destination;
 - determining whether the amount of the data is uncharacteristically high; and
 - performing a corrective action if the amount of the data is uncharacteristically high.
15. (Original) The method of claim 14, wherein the corrective action comprises blocking the data transfer.
16. (Currently amended) The method of claim 14, wherein the corrective action comprises disabling the program that requested the outgoing transfer of data.
17. (Original) The method of claim 14, wherein the step of performing a corrective action comprises:
- changing the destination of the outgoing transfer to the computer system; and
 - determining whether the program operates in response to the changed destination.
18. (Original) The method of claim 14, wherein the step of performing a corrective action comprises:
- irreversibly encrypting the data; and
 - determining whether the program operates in response to the encryption.
19. (Original) The method of claim 18, wherein the step of irreversibly encrypting the data comprises injecting random numbers into the data.

20. (Original) The method of claim 14, further comprising:
determining whether the data includes personal information; and
performing a corrective action if the data includes personal information.
21. (Original) The method of claim 20, wherein the step of determining whether the data includes personal information comprises performing a text string search or binary pattern search on the data.
22. (Original) The method of claim 14, wherein the step of performing a corrective action comprises storing a log of the outgoing transfer.
23. (Original) The method of claim 22, wherein the step of storing a log of the outgoing transfer comprises storing the data.
24. (Original) The method of claim 22, further comprising transferring the log to a remote computer.
25. (Currently amended) An apparatus for monitoring data sent from a computer system, comprising:
detection means for detecting a request for an outgoing transfer of data from a program in the computer system to a destination;
determination means for determining whether the destination is a trusted site; and
correction means for performing a corrective action if the destination is not a trusted site;
means for determining whether the data includes personal information if the destination is a trusted site; and
means for performing the corrective action if the data includes personal information.
26. (Original) The apparatus of claim 25, wherein the determination means comprises means for matching the destination against a list of trusted sites.

27. (Original) The apparatus of claim 25, wherein the corrective action comprises blocking the outgoing transfer.
28. (Currently amended) The apparatus of claim 25, wherein the corrective action comprises disabling the program that requested the outgoing transfer of data.
29. (Original) The apparatus of claim 25, wherein the correction means comprises:
means for changing the destination of the outgoing transfer to the computer system; and
means for determining whether the program operates in response to the changed destination.
30. (Currently amended) The apparatus of claim 25, wherein the correction means comprises:
encryption means for ~~irreversibly~~ encrypting the data; and
means for determining whether the program operates in response to the encryption.
31. (Currently amended) The apparatus of claim 30, wherein the encryption means comprises means for irreversibly encrypting the data by injecting random numbers into the data.
32. (Original) The apparatus of claim 25, further comprising:
means for determining whether the amount of data for the outgoing transfer is uncharacteristically high; and
means for performing a corrective action if the amount of data is uncharacteristically high.
33. (Cancelled)

34. (Currently amended) The apparatus of claim ~~33~~ 25, wherein the means for determining whether the data includes personal information comprises means for performing a text string search or binary pattern search on the data.
35. (Original) The apparatus of claim 25, wherein the step of performing a corrective action comprises storage means for storing a log the outgoing transfer.
36. (Original) The apparatus of claim 35, wherein the storage means comprises means for storing the data.
37. (Original) The apparatus of claim 35, further comprising means for transferring the log to a remote computer.
38. (Original) An apparatus for monitoring data sent from a computer system, comprising:
detection means for detecting a request for an outgoing transfer of data from a program in the computer system to a destination;
determination means for determining whether the amount of the data is uncharacteristically high; and
correction means for performing a corrective action if the amount of the data is uncharacteristically high.
39. (Original) The apparatus of claim 38, wherein the corrective action comprises blocking the data transfer.
40. (Currently amended) The apparatus of claim 38, wherein the corrective action comprises disabling the program that requested the outgoing transfer of data.
41. (Original) The apparatus of claim 38, wherein the correction means comprises:
means for changing the destination of the outgoing transfer to the computer system; and

instructions for detecting a request for an outgoing transfer of data from a program in the computer system to a destination;

instructions for determining whether the destination is a trusted site; ~~and~~

instructions for performing a corrective action if the destination is not a trusted site;

instructions for determining whether the data includes personal information; and

instructions for performing a corrective action if the data includes personal information.

50. (Original) A computer program product, in a computer readable medium, for monitoring data sent from a computer system, comprising:

instructions for detecting a request for an outgoing transfer of data from a program in the computer system to a destination;

instructions for determining whether the amount of the data is uncharacteristically high; and

instructions for performing a corrective action if the amount of the data is uncharacteristically high.